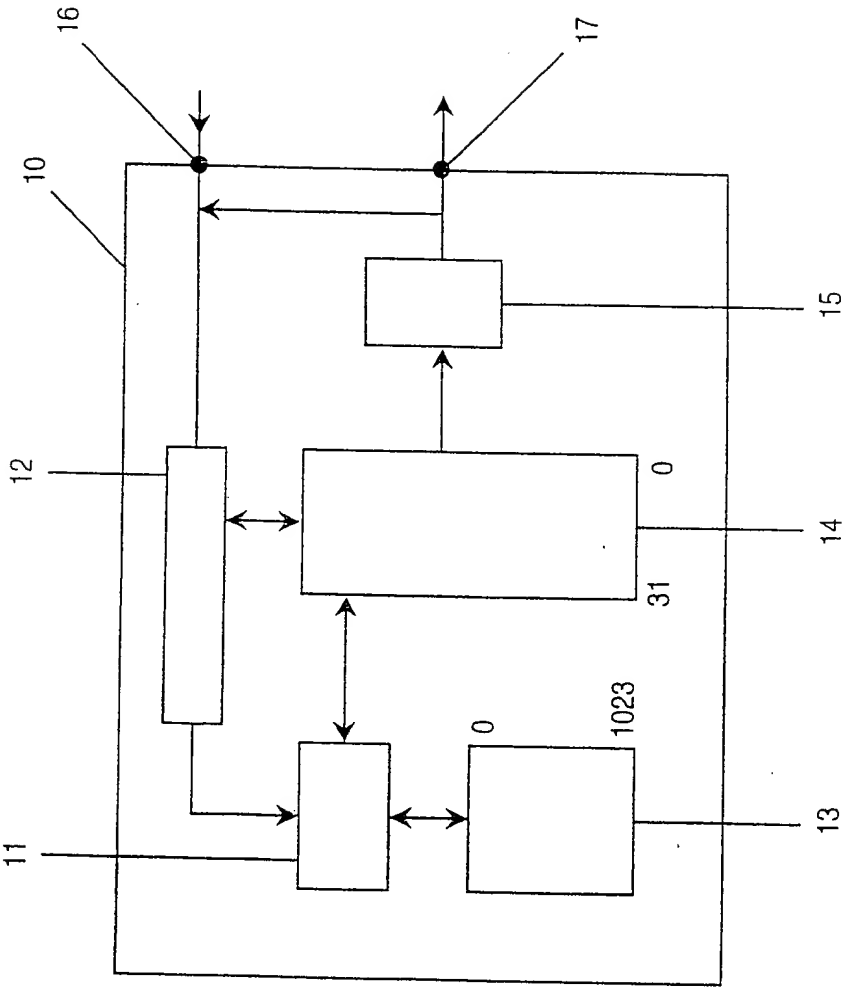

Fig.1

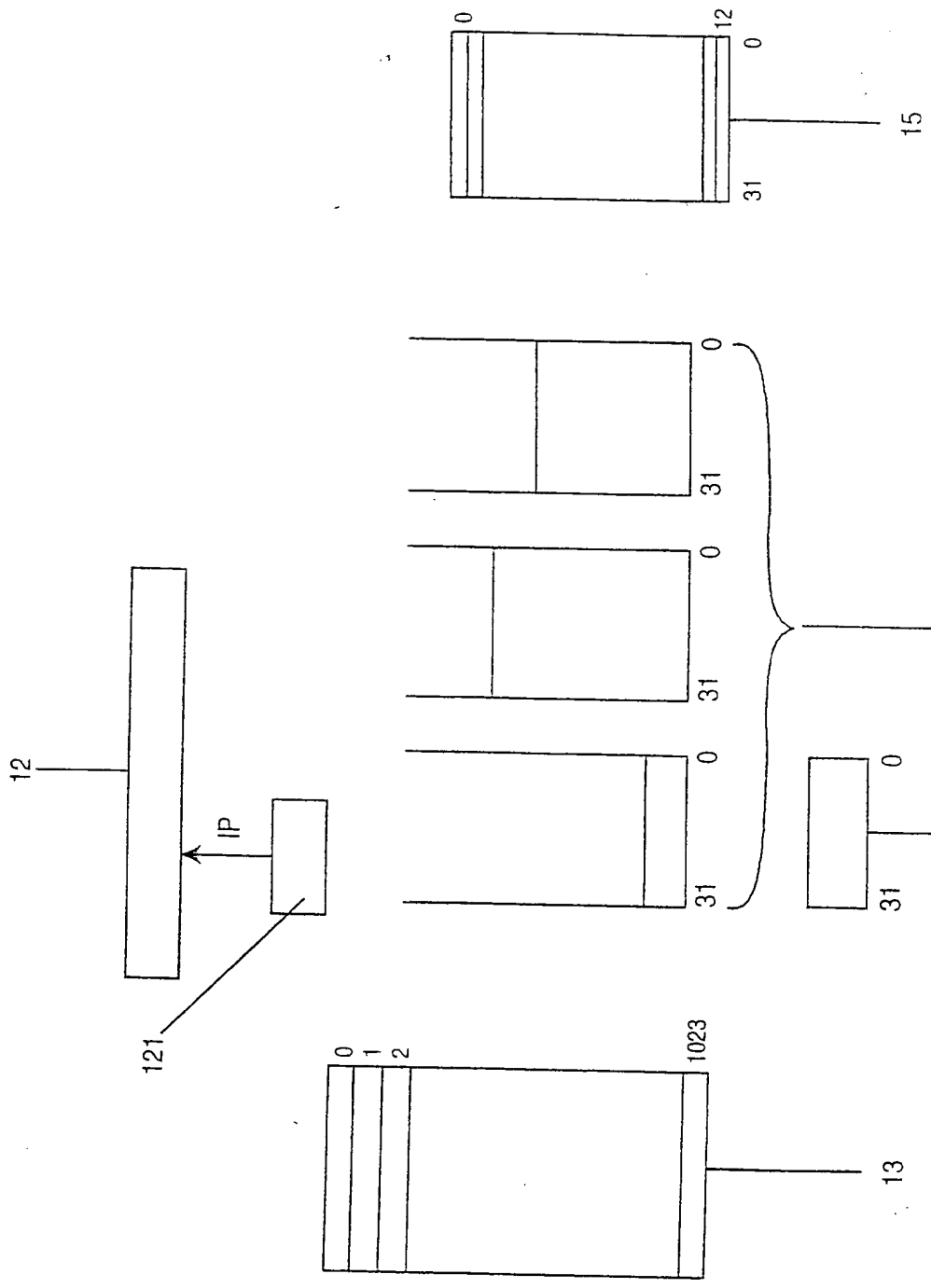

Fig.2

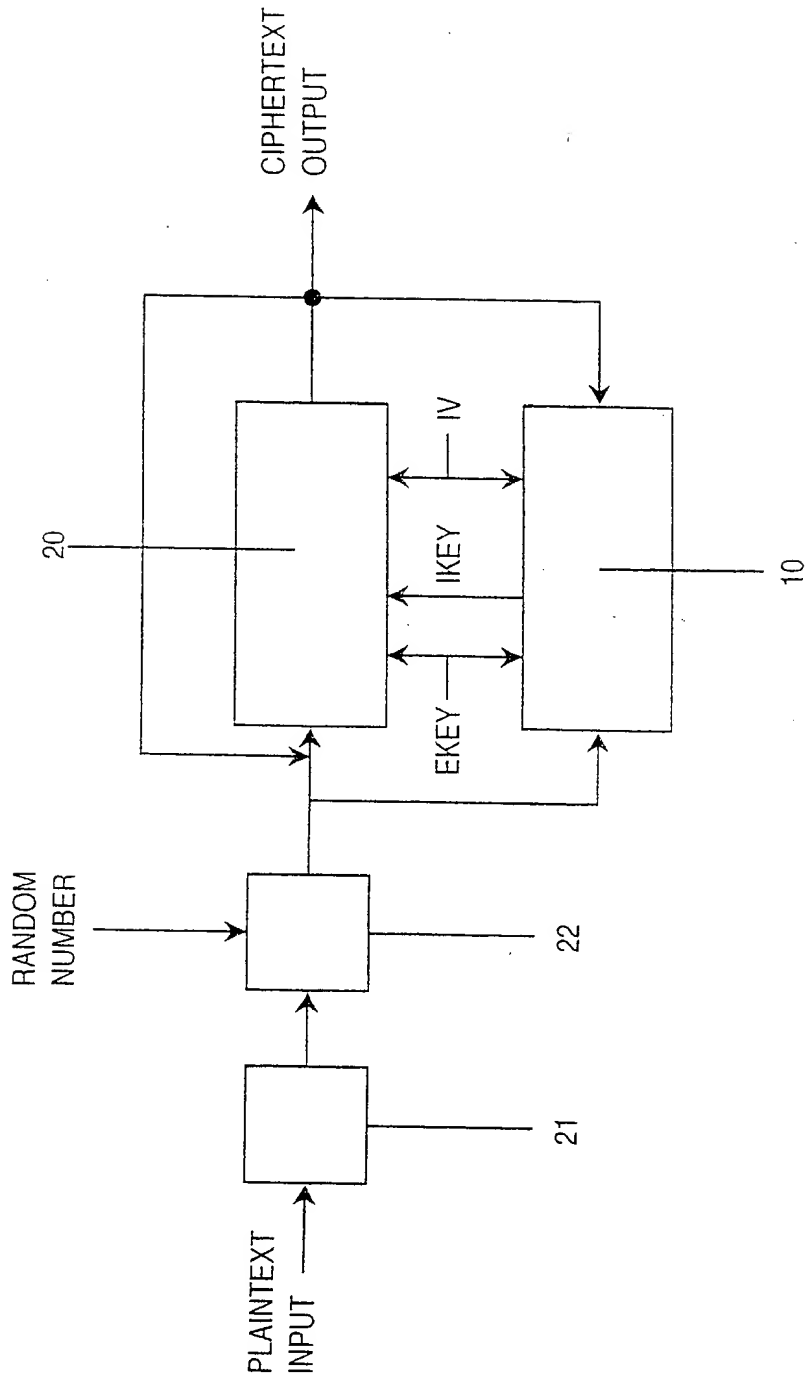
CIPHERTEXT
OUTPUT
IV
IKEY
EKEY
20
10
RANDOM
NUMBER
22
21
PLAINTEXT
INPUT

Fig.3

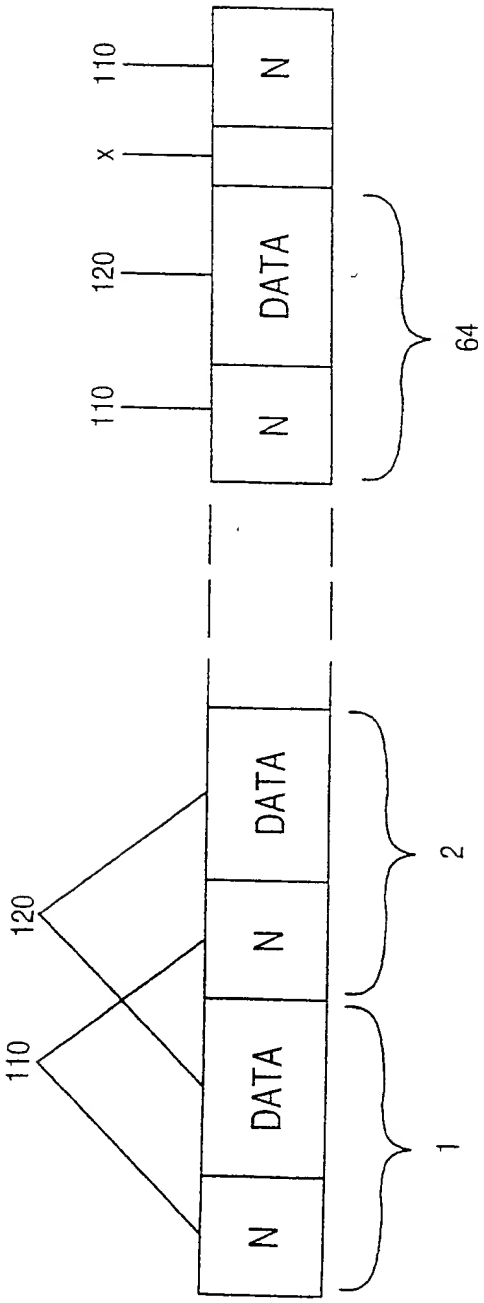

Fig.4

Fig.5

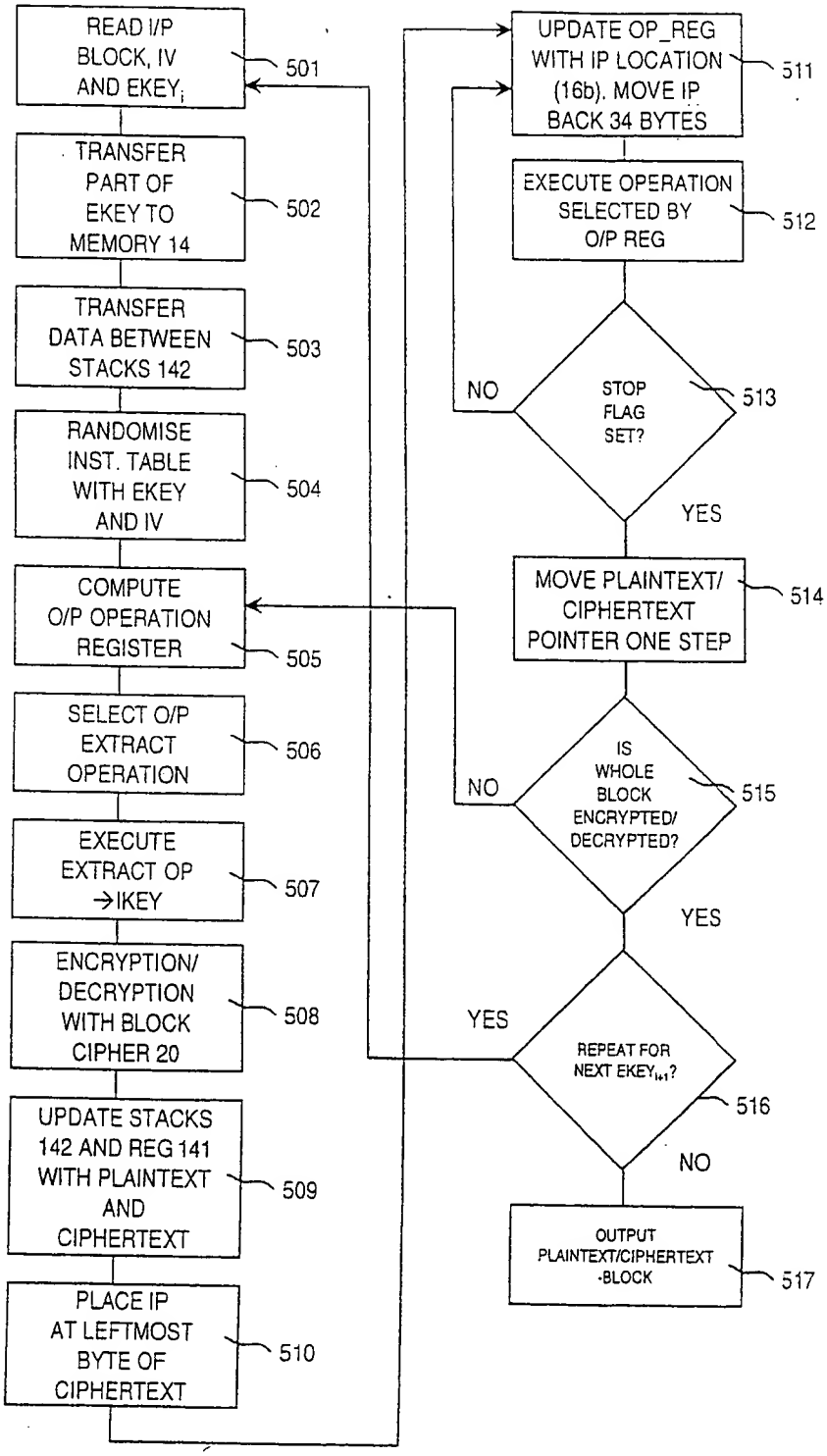

Fig.6

WO 96/09694 PCT/GB95/02182

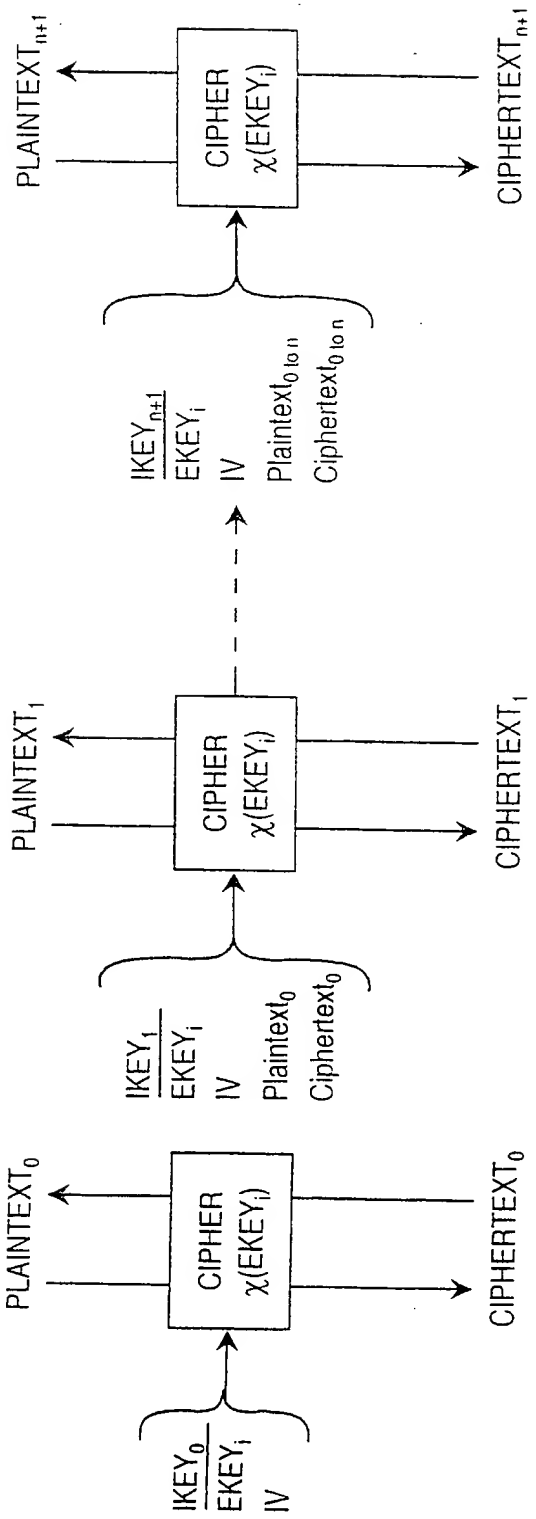
PLAINTEXT$_{n+1}$
CIPHER
χ(EKEY$_i$)
CIPHERTEXT$_{n+1}$
IKEY$_{n+1}$
EKEY$_i$
IV
Plaintext$_{0\ to\ n}$
Ciphertext$_{0\ to\ n}$
PLAINTEXT$_1$
CIPHER
χ(EKEY$_i$)
CIPHERTEXT$_1$
IKEY$_1$
EKEY$_i$
IV
Plaintext$_0$
Ciphertext$_0$
PLAINTEXT$_0$
CIPHER
χ(EKEY$_i$)
CIPHERTEXT$_0$
IKEY$_0$
EKEY$_i$
IV

Fig.7

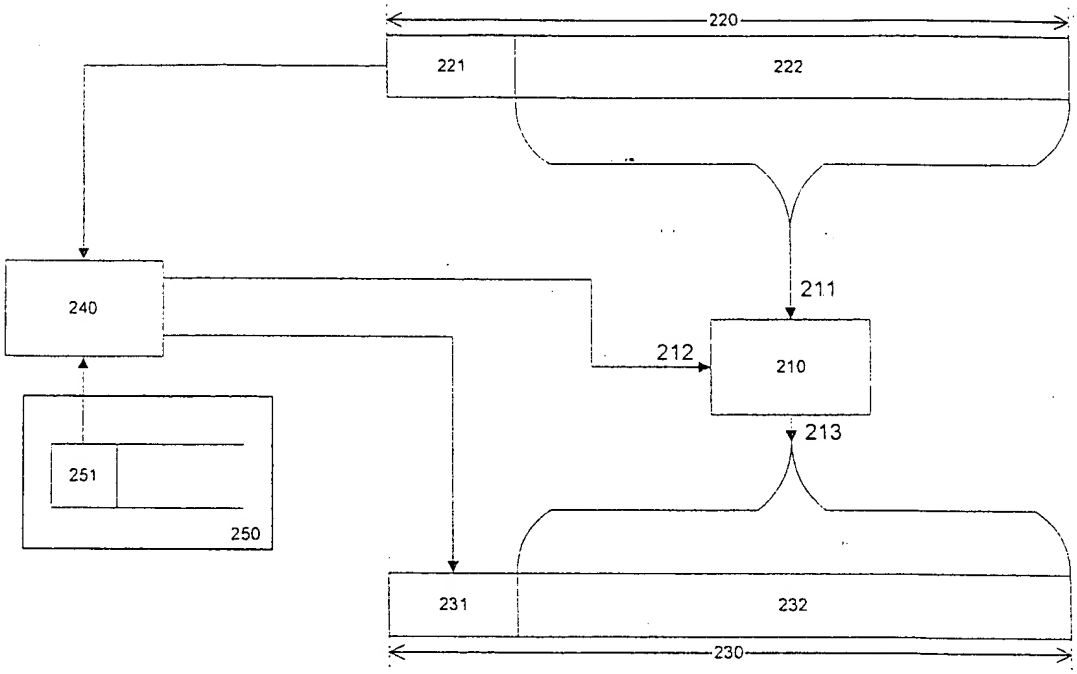
220
221
222
240
211
212
210
213
251
250
231
232
230

FIG.8

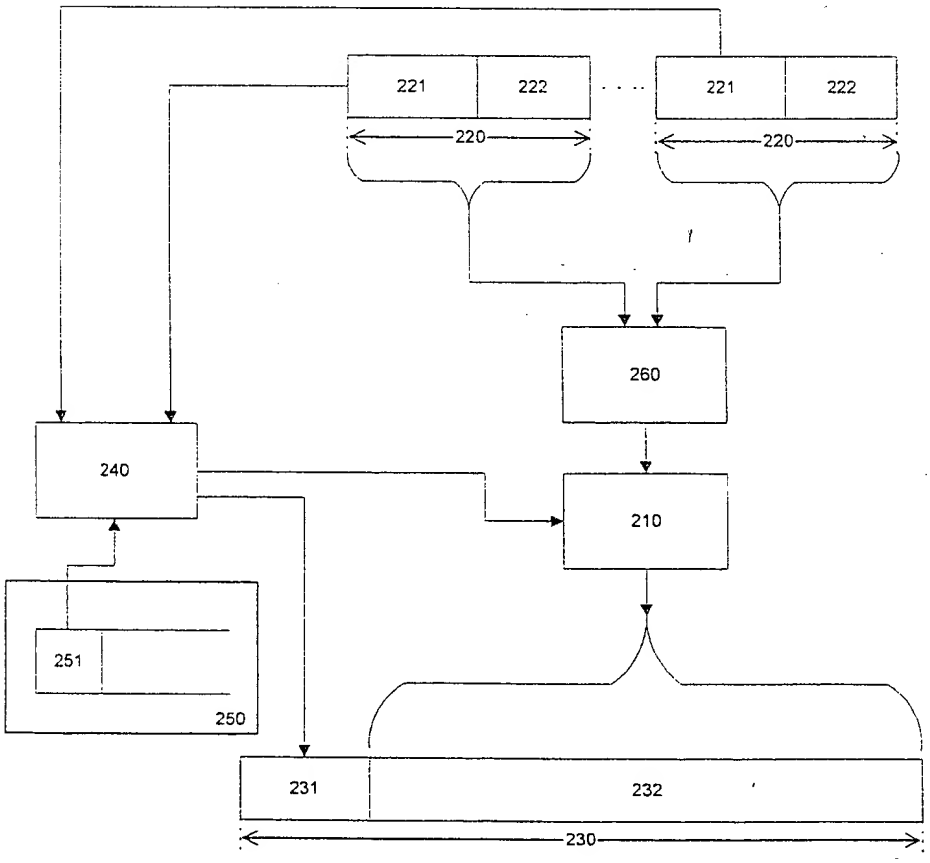
221
222
221
222
220
220
260
240
210
251
250
231
232
230

FIG.10

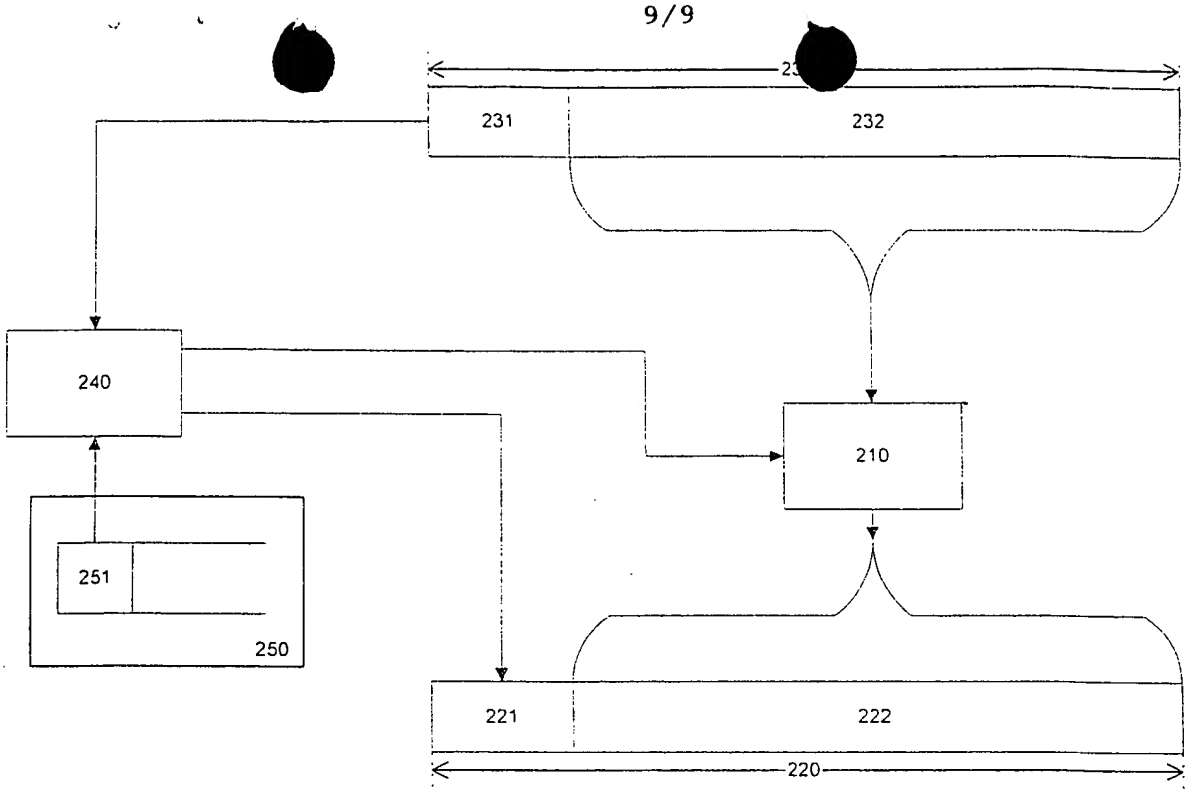
231
232
240
210
251
250
221
222
220

FIG.9

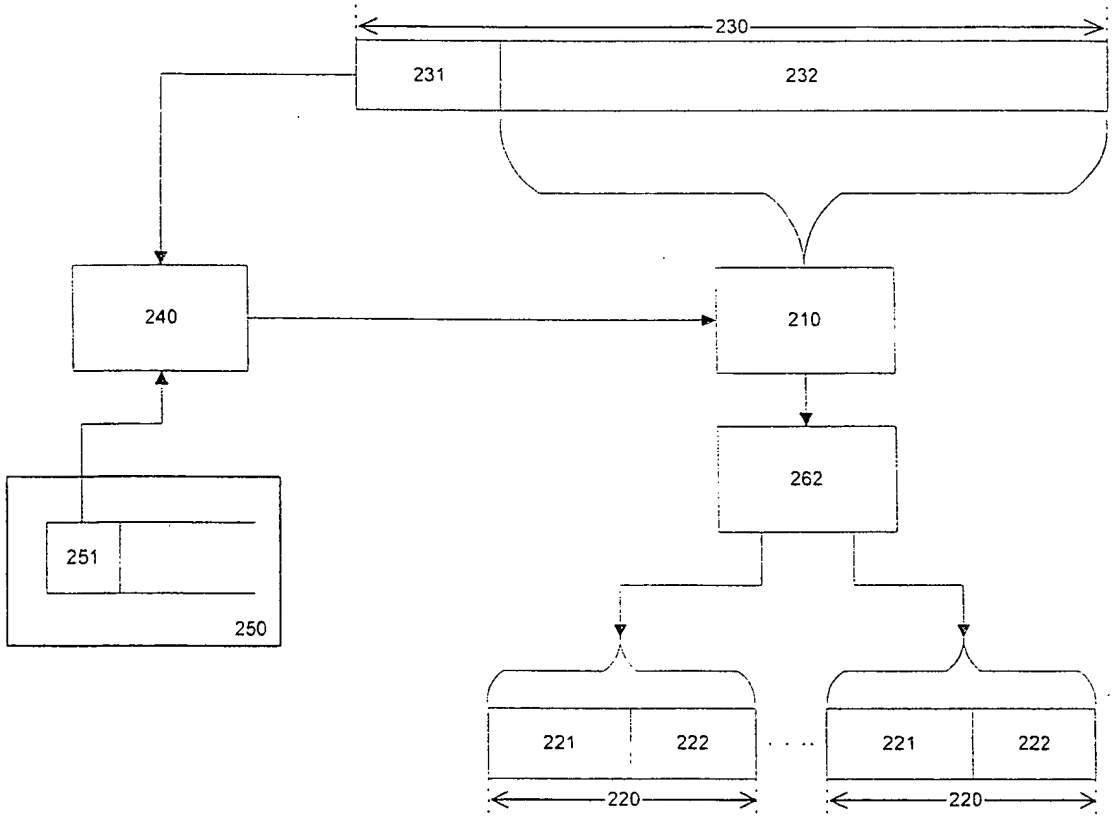
230
231
232
240
210
262
251
250
221
222
221
222
220
220

FIG.11